EXECUTIVE SUMMARY

What will happen when the clock strikes midnight on December 31, 1999? A single, specific answer to that question is still unknown (and, ultimately, unknowable) but the extensive information developed by the Committee and outlined in this report provides an understanding of the size, scope, and nature of the problems that may occur.

There is currently widespread awareness that Y2K involves more than the failure of an individual's personal computer, or an incorrect date in a spreadsheet. Potential Y2K problems increase exponentially upon examination of the multiple layers of computer systems, networks and technologies supporting individuals' everyday lives. It is now widely understood that Y2K could affect the lives of individuals, but exactly in what manner is unknown.

Inherent uncertainty in the outcome of Y2K fuels public concern and makes preparation difficult. Sensationalists continue to fuel rumors of massive Y2K failures and government conspiracies, while some corporations and nations concerned about their image downplay real Y2K problems. The Committee finds that both extremes are counterproductive, and do not accurately reflect what typifies most Y2K problems. The true extent of Y2K failures will match neither the most optimistic nor the most apocalyptic predictions. Rather, Y2K problems will hit sporadically, based on geography, size of organization, and level of preparedness, and will cause more inconveniences than tragedies.

While optimism pervades the domestic Y2K outlook, uncertainty with regard to Y2K's impact dictates that preparation is prudent. Individuals and companies must take charge of their own situation by examining the Y2K readiness of the utilities and services that they depend on, and by preparing accordingly.

In the past 14 months, companies and nations, large and small, have taken the Y2K problem seriously. The increase in worldwide public awareness, remediation, and contingency planning since the Committee's February 1999 report, "Investigating the Impact of the Year 2000 Problem," has been remarkable. However, the Committee's hearings, interviews, and research reveal that many organizations and industries remain unprepared. The Y2K problem still has the potential to be very disruptive, necessitating continued, intensive preparation in the time remaining. Y2K risk management efforts must be increased to avert serious disruptions.

While the Committee has become increasingly confident about U.S. Y2K preparedness, it has become increasingly concerned about international Y2K preparedness. Some of our important trading partners are months behind in addressing the Y2K problem and are not likely to avoid significant disruptions. These

disruptions could have adverse economic effects here at home and, in some developing countries, result in requests for humanitarian assistance.

OVERALL OBSERVATIONS

Sectors critical to the safety and well-being of Americans, as well as to the economy, have made significant progress in the last eight months; concerns remain in health care, local governments, small business, and education.

Most physicians' offices, many inner-city and small rural hospitals, and numerous nursing homes have not fully addressed the Y2K problem. In general, larger firms have grasped how a Y2K failure could severely impact their businesses and are taking steps to remedy the problem. Unfortunately, nearly half of small- and medium-sized businesses across all sectors are taking a wait-and-see approach to Y2K.

Many local governments and some public safety answering points used to process 911 calls remain at risk of Y2K disruptions; as of June 1999, only 37% points were compliant. Most school districts, colleges, and universities are not prepared; surveys this summer indicate that less than one-third were Y2K ready.

Many projected Y2K readiness deadlines are dangerously late.

Heightened concern exists with regard to organizations and industries that project readiness dates in the last quarter of 1999. For example, approximately 500 of the 8,000 oil and gas companies--and 30 of the 103 nuclear power plants--project completion dates after September 30, 1999. Original completion dates were planned in the first quarter to allow plenty of time to complete end-to-end testing and to address unexpected anomalies. However, these projected completion dates continue to be deferred. Organizations with late completion dates are not leaving sufficient time to address unexpected problems, which also heightens the importance of adequate contingency planning.

Pandemic self-reporting may result in overly optimistic Y2K projections.

Self-reporting, which is analogous to letting students grade their own tests, offers data of varying reliability. Nonetheless, self-reporting has become the standard in private industry and government, both domestically and internationally. Since its last report, the Committee has seen a trend toward greater use of independent verification, but self-reported surveys are still the most widely utilized tools to measure Y2K readiness and predict success.

Y2K disclosures remain inadequate.

The Year 2000 Information Readiness and Disclosure Act (Public Law No. 105-271) provided a basic level of protection for Y2K statements made in good faith. The CRASH Protection Act of 1997 (S.1518, 105th Congress) pressured the Securities and Exchange Commission (SEC) to

require more meaningful Y2K corporate disclosure to shareholders.

Despite the SEC rule requiring Y2K disclosure by public corporations, companies are reluctant to report compliance levels, for fear of litigation or ceding competitive advantage. In August 1999, the SEC fined nine investment entities for failure to adequately disclose Y2K readiness information.

National emergency planning for Y2K-related failures is evolving.

The Federal Emergency Management Agency (FEMA) continues to refine plans to handle Y2K-related emergencies. However, state and local governments represent the first line of defense in emergency situations, and emergency planning varies widely at these levels.

In addition, organizations are charged with the responsibility of developing adequate contingency plans in the event that Y2K-related disruptions do occur. Some sectors have achieved greater progress in this regard than others.

Finally, the Administration plans to develop a Y2K Information Coordination Center (ICC) to monitor and address Y2K problems nationwide. It is unclear how the ICC will function, since participation and reporting details essential to its viability and effectiveness are as yet undetermined.

The international Y2K picture is more disturbing.

The Y2K preparations in many countries of economic and strategic importance to the U.S. are inadequate. Of greatest concern are Russia, China, Italy, and several oil-producing countries. The Y2K problem has highlighted the economic interdependence of nations. A significant potential exists for the Y2K-induced problems of other nations to wash up on our shores--whether in the form of recession, lost jobs, or requests for international assistance.

The Y2K problem highlights cyber vulnerabilities.

Study of the Y2K issue has heightened awareness of vulnerabilities in America's high-tech infrastructure. Millions of lines of computer code have been sent overseas for Y2K repair. This creates the possibility that those wishing to commit acts of terrorism or political and corporate espionage could use “trap doors” or “logic bombs”.

In the current information age, attacks on American defense and industrial facilities in cyberspace are as real and dangerous as conventional threats to economic prosperity and national security. The Committee recommends the development of a national policy to protect private industry's high-tech infrastructure and safeguard the federal government's ability to meet the defense challenges of the next millennium.

SECTOR ASSESSMENTS

Since its establishment in April 1998, the Committee has held nearly 30 hearings, received testimony from more than 150 witnesses, written numerous letters, participated in forums and working group meetings, held multiple "town hall" meetings, and talked to hundreds of experts. Shortly after its inception, the Committee set forth the following critical sectors for study, listed in order of their importance:

- Utilities
- Healthcare
- Telecommunications
- Transportation
- Financial Services
- General Government
- General Business
- Litigation

To these original eight sectors, the Committee has added the sectors of international preparedness and personal preparedness. A summary of the Committee's assessments, expectations, and concerns in each of these sectors follows.

The Committee's ratings of these sectors are provided in the table on page 9. The ratings are based on five risk factors—preparedness status, data quality, public disclosure, contingency planning, and dependencies.

UTILITIES

A prolonged, nationwide blackout will almost certainly not occur; that is, the power grid will work. However, local and regional outages remain a distinct possibility depending upon the readiness of the 3,000 utilities serving any given area. Further clouding accurate assessment, only 25% of electric utilities routinely disclose Y2K information to the public, making it difficult for individuals and organizations to get detailed information on "their" utilities. While bulk power producers, including nuclear facilities, are generally well prepared, they still must develop comprehensive contingency plans to prepare for unexpected problems.

Oil and gas companies have made notable advances since the Committee's last report, but continued progress remains essential. Nearly 500 companies do not plan to complete repairs until late 1999, which makes disruption possible for some domestic oil and gas billing, production, transportation, and distribution. In addition, the likelihood of disruption in oil imports is high due to the lack of preparedness in key oil-producing countries. Disruptions could ultimately affect gas prices and availability.

The enormous scope and variation in the use of technology in the water industry makes it difficult to generalize. However, our assessment of the water industry is generally positive. The Environmental Protection Agency and professional associations have waged a very aggressive readiness campaign. On the other hand, while a recent survey on the readiness of wastewater facilities expressed a high degree of confidence, it also indicate that much work remains to be done to ensure readiness. A joint study conducted

by the major water treatment associations concluded that, while isolated malfunctions in equipment could occur, interruptions in service should be limited in scale and of short duration.

HEALTHCARE

Y2K compliance is mixed in the healthcare industry, which is characterized by extensive decentralization of operations. Some segments, such as pharmaceutical manufacturing, wholesaling and distribution, and large-scale hospitals, have invested the managerial and financial resources to remediate and test for most Y2K problems. Conversely, rural and inner city hospitals, nursing homes, and physicians' offices have particularly high Y2K risk exposure due to limited technical/managerial resources and lack of awareness.

The Committee remains concerned about the hundreds of different types of electronic biomedical devices used by all healthcare providers. Most in the medical device industry have identified the Y2K compliance of their products, but end-to-end testing within a facility has not been the norm. The difficulty in testing and limited resources available for replacement of devices at some institutions contributes to the Committee's concern and raises serious patient safety questions.

Healthcare is the nation's single largest industry, generating $1.5 trillion annually. The U.S. has 6,000 hospitals, 800,000 doctors in 50,000 offices, and 16,000 nursing homes, as well as 2,000 biomedical equipment manufacturers and numerous healthcare insurers in the public (Medicare/Medicaid) and private sectors. All of these entities are highly automated and, thus are highly exposed to Y2K risk. On a positive note, the Health Care Financing Administration, the federal agency that oversees Medicare payments, has made a nationwide effort to ensure that its health claims payments system is Y2K compliant.

TELECOMMUNICATIONS

The telecommunications industry has spent billions of dollars on Y2K fixes and, in August 1999, reported that 98% of the industry was ready. As a result, carriers project minimal service disruptions domestically. Internationally, however, there could be problems in completing calls to some high-risk countries. International telecommunications carriers are working to develop an international early warning system to share Y2K information.

Still, unpredictable infrastructure failures, sudden changes in consumer behavior, or customer premise equipment and private network problems could adversely impact telecommunications. Increased call volume and ad hoc "testing" could congest networks and erode stability. Full interoperability between compliant and non-compliant elements and their impact on the public switched network remains unknown. The lagging Y2K readiness of small and medium-sized domestic carriers could impact services in rural communities. Finally, there has been no attempt to assess whether the rush to implement Y2K fixes on a global scale will having a lingering impact

on the stability of global communications networks over the next year.

The Committee remains concerned about customer premise equipment—the telephone equipment used to route calls within most businesses. Failed customer premise equipment could have a severe impact on business operations if not adequately addressed.

TRANSPORTATION

Transportation is the linchpin for just-in-time inventory management across almost every business sector, from healthcare supplies to food.

The Federal Aviation Administration has successfully completed its effort to make the nation's air traffic control systems ready. Notwithstanding this considerable progress, it appears that some of the nation's 670 domestic airports remain at risk in areas such as jetway security systems and runway lighting. It is likely there will be disruptions resulting in delays at some U.S. airports. The situation with international air traffic control and airports is much more worrisome.

The maritime shipping industry has not moved aggressively toward compliance, leading to the likelihood of disruptions in global trade.

Many public transit systems have also failed to aggressively address the Y2K problem, which makes service disruptions likely for some transit systems. Most transit authorities plan to suspend bus and railcar operations for a brief period around midnight on December 31, 1999, as a safety precaution.

FINANCIAL SERVICES

The financial services sector in the U.S. will be prepared for the millennium date change. Automatic teller machines are expected to function correctly, and banks should have adequate cash to meet consumer demand, based on a Federal Reserve estimate that each American household will withdraw an average of $500. Federal regulators have made considerable progress in tracking compliance among banks, thrifts, and credit unions, 99% of which have received satisfactory government ratings. Regulators are encouraging financial institutions to communicate their preparedness to customers in order to reduce the potential for panic.

The securities industry has responded well to its internal Y2K issues and has undertaken expansive testing. However, fund managers and brokers have only recently started to consider the implication of corporate Y2K vulnerability on investment decisions.

GENERAL GOVERNMENT

The federal government will spend in excess of $8 billion on Y2K. Wholesale failure of federal government services is not likely to occur. In addition, FEMA is now engaged in national emergency planning in the event of major and minor Y2K disruptions. State and local government preparedness remains a concern for the Committee.

There is wide variation in the Y2K readiness of the nation's 50 states, 3,066 counties, and 87,000 local jurisdictions. Several states and many local governments lag in Y2K remediation, raising the risk of service disruption. For example, approximately 10 states are not prepared to deliver such critical services as unemployment insurance and other benefit payments. Surveys indicate that 65% of state critical systems were ready as of May 1999, and only 25% of counties reported being ready as of June 1999. Of greatest concern at the local level is the readiness of the 911 Public Safety Answering Points, and the ability to provide adequate response in the face of a potential increase in demand for service due to Y2K problems.

GENERAL BUSINESS

In general, large companies with greater resources have dealt well with the Y2K problem. Very small businesses may survive using manual processes until Y2K problems are remediated. However, many small- and medium-sized businesses are extremely unprepared for Y2K disruptions. One survey shows that 28% of small businesses do not plan to take any action.

The heavily-regulated insurance, investment services, and banking industries are farthest ahead in their efforts; healthcare, oil, education, agriculture, farming, food processing, and the construction industries are lagging behind. The cost to regain lost operational capability for any mission-critical failure will range from $20,000 to $3.5 million, with an average of 3-15 days necessary to regain lost functions.

LITIGATION

The prospect of litigation arising from Y2K-related failures has overshadowed the Committee's information gathering from its inception. Early estimates placed litigation costs as high as $1 trillion. Along with the Senate Committees on Commerce and the Judiciary, the Committee held a hearing to examine the potential Y2K litigation explosion, and assisted in the drafting of legislation to address the issue. Senator Dodd played a key role in the passage and enactment of the Y2K Act (Public Law No. 106-37), which is intended to encourage remediation of Y2K problems instead of litigation.

INTERNATIONAL

The Committee is greatly concerned about the international Y2K picture. Several countries of strategic and economic importance to the U.S. are severely behind in Y2K remediation efforts. Regions of the world of most concern to the Committee are Eastern Europe, Africa, and parts of Asia and South America. When considering strategic and economic factors, and the status of Y2K remediation efforts within specific countries, the Committee's greatest concerns lie with China, Russia, Italy, and several of the countries from which the U.S. imports oil.

Severe long- and short-term disruptions to supply chains are likely to occur. Such disruptions may cause a low-to-moderate downturn in the economy, particularly in those in-

dustries that depend on foreign suppliers. In addition, there may be a request for humanitarian relief from developing countries that have not addressed the Y2K problem.

PERSONAL PREPAREDNESS

Communities and individuals should take reasonable steps to prepare for the Year 2000. Consumers are urged to keep copies of financial statements and to ask local banks what efforts are being made toward Y2K compliance. Individuals should research companies' compliance levels before making investment decisions. The Y2K problem has been likened to a winter storm, with the implication that similar preparation is appropriate. With their individual circumstances in mind, Americans should prepare for Y2K based on facts and reasonable predictions about the problem's effects on vital services.

* * * * * *

The challenges posed by the Y2K problem are numerous and daunting. The Committee conducted extensive research and held numerous hearings in 1999, but still cannot conclusively determine how extensive Y2K disruptions will be. However, the Committee has no data to suggest that the U.S. will experience nationwide social or economic collapse. Nonetheless, disruptions will occur and in some cases those disruptions will be significant. The international situation will certainly be more tumultuous

.

Y2K SECTOR RISK EXPOSURE ASSESSMENTS

SECTOR	Progress (1)	Data Quality (2)	Disclosure (3)	Contingency planning (4)	Dependency (5)	*Overall quality*
Utilities						★★★★
Electric Utilities	●	◕	◑	◑	◕	
Oil & Gas Utilities	◑	◑	◒	◕	◒	
Water Utilities	◕	◑	◕	●	◒	
Health Care						★★
Prescription Drugs	◕	◕	◕	◕	◑	
Urban-Suburban Hospitals	◑	◑	◒	◑	○	
Rural & Inner City Hospital	○	○	◒	◒	○	
Health Claims Billing System	◑	◕	◕	◒	○	
Physicians Offices	○	○	◑	○	○	
Nursing Homes	○	○	◒	◒	○	
Telecommunications	●	◑	◕	◑	◒	★★★★
Transportation						★★★
Aviation	◕	○	◑	●	○	
Maritime Shipping	◕	○	◑	●	○	
Railroads	◒	◒	◑	◑	◕	
Public Transit Systems	◒	○	◕	◕	◕	
Automobiles, Trucks, & Traffic Control	●	○	◕	◑	◕	
Financial Services	●	●	◕	◕	◒	★★★★★
Government Services						★★★
Federal Agencies	◕	◕	◕	◑	◕	
State and Local Government	◒	○	◒	○	◒	
Emergency Preparedness/ Response	◑	◒	◕	◕	●	
Business						★★★
Small to Medium Sized Businesses	◕	○	◒	◑	◕	
Global Corporations	◕	◒	◑	◕	◒	
Food Supply	◕	◑	◑	◕	◑	
Chemical Industry	◒	○	○	◕	◒	
International						★★
Africa	◒	◑	○	◒		
Asia	◑	◑	◒	◑		
Eastern Europe	○	◑	◑	◒		
Latin America	◒	◑	◑	◑		
Western Europe	◑	◕	◕	◕		

(1) Performance of sector in meeting deadlines for remediation, testing, and planning
(2) Quality and scope of the data that is available for evaluation
(3) Transparency and public disclosure of information
(4) Contingency planning and preparedness
(5) Dependency on externalities, including international supply chains

Legend

○ High exposure
◒ Above average exposure
◑ Average exposure
◕ Below average exposure
● Low exposure
★'s are awarded for lower ris